In the Claims

Please amend Claim 1. Rest of the claims remains same (they being dependent claims).

1. (Currently amended) A method of authenticating a transaction, the method comprising:

causing a separate unit to communicate with a device,

the separate unit being secured and independently operating from the device, the separate unit configurable to include a ~~first~~ biometric sensor to obtain ~~first~~ biometric characteristics of a user, the ~~first~~ biometric characteristics physically representing the user;

initiating a local authentication process~~,~~ using the separate unit, the local authentication process comprising:

~~and its biometric sensor to~~ obtaining the biometric characteristics of ~~a~~ the user from the biometric sensor;

decrypting stored biometric characteristics for the user; and

~~by~~ comparing the biometric characteristics with ~~pre-configured and~~ the stored biometric characteristics; ~~in a smartcard located in a smartcard reader located inside the separate unit;~~

if the biometric characteristics match with the stored biometric characteristics, initiating an encrypted authentication transaction request comprising:

receiving personalized data at the device from the user;

recovering atomic time for usage in session key generation;

encrypting the personalized data using the sessions keys, public keys and third party public keys; and

sending the encrypted personalized data to the third party through the device as encrypted authentication transaction request using a challenge response protocol method, wherein the atomic time is used as a serialization and challenge response protocol variable;

~~initiating an encrypted authenticated transaction request where personalized data is encrypted using said biometric characteristics as well as atomic clock where the atomic clock is used as serialization and challenge response protocols variable, and generating unique sessions keys~~

~~used as private keys as well as personalized data used as public key using the device to send this encrypted authenticated transaction request using a challenge response protocol method;~~

~~communicating the encrypted authenticated request to a third party through the device; and~~

receiving a signal at the separate unit signing the encrypted authenticated transaction request via the device to authenticate the transaction; and

~~such authentication being done locally in the separate unit without the use of any central server, wherein the separate unit is cause to request personalized data from the user associated with the device, the separate unit is not to encrypt the transaction but to~~

digitally sign<u>ing</u> the authentication <u>at the separate unit</u> using the atomic time clock stamping of the transaction between the device and the third party. ~~only when the biometric characteristics of the user is verified, the transaction can only be authenticated when the personalized data is authenticated in the separate unit.~~

2. (Previously presented) The method of claim 1, wherein the separate unit is further configurable to include a second biometric sensor to acquire second biometric characteristics of the user to ensure that the user is indeed authenticated.

3. (Previously presented) The method of claim 1, wherein the first biometric sensor is a fingerprint sensor to acquire a fingerprint of the user, and the second biometric sensor is a microphone to acquire a voice of the user.

4. (Original) The method of claim 1, wherein the device is a personal digital assistant (PDA).

5. (Original) The method of claim 1, wherein the device is a telephone.

6. (Original) The method of claim 5, wherein the telephone is a cellular telephone.

7. (Original) The method of claim 1, wherein the signal used to authenticate the transaction is a high-contrast signal.

8. (Previously presented) The method of claim 1, wherein said communicating the transaction request to the third party involves a use of a dual tone audio signal.

9. (Original) The method of claim 1, wherein the signal is an audio frequency shift keying (AFSK) signal.

10. (Original) The method of claim 8, wherein the signal is an audio frequency shift keying (AFSK) signal.

11. (Previously presented) The method of claim 8, wherein the signal is a private line (PL) signal or a wireless signal.

12. (Previously presented) The method of claim 1, wherein said initiating a transaction request includes an entry of a personal identification number (PIN) through the keyboard of the device.

13. (Previously presented) The method of claim 12, wherein the separate unit is terminated if a PIN entry is attempted more than a predetermined number of times.

14. (Previously presented) The method of claim 1, wherein the separate unit further includes a biometric input; and said initiating a transaction request includes receiving biometric data through the biometric input.

15. (Original) The method of claim 14, wherein the biometric input is a fingerprinting.

16. (Previously presented) The method of claim 1, wherein one or both of the transaction request and the authentication signal are encrypted.

17. (Previously amended) The method of claim 16, wherein the encryption is based on public key cryptography further including and not limited to Identity-Based Encryption (IBE).

18. (Previously presented) The method of claim 1, wherein the separate unit or device includes a memory; the transaction request and authentication signal constitute a session; and information regarding the session is stored in the memory.

19. (Previously presented) The method of claim 1, wherein the separate unit is a headset.

20. (Previously presented) The method of claim 19, wherein the headset includes capability of reading in confidential information from a user associated with the device.

21. (Previously presented) The method of claim 1, wherein the said encryption is performed using a one-way encryption algorithm that employs one or many biometric input, atomic clock and unique session keys.

22. (Previously presented) The method of claim 1, wherein the said authentication is performed using a challenge response protocol.